

PRACTICAL PARANOID'S

BOOK OF ENCRYPTION

AND OTHER RELATED

SUBJECTS

BY

HOMER OTTO GOODALL, JR

Many books on this subject are written by so called experts and only use the theory and practice they had learned from a book. This book was taken from real life experience. The reader will learn what will work and what will not work. I bow to no higher power than does it work. These techniques take time to learn, but they can save a person a great deal of trouble.

Encryption layering was learned when I found out by a rumor being started by someone that I had illegal files on my system. I began to look for software that I could search my computer for the illegal files, but the deletion of these files was difficult. The person had put a sticky virus on them and they were treated as system files. I found out the children that put their pictures on the system. I knocked on their door and they were shocked that I found out their identity. I had seen them hanging around the library and recognized them. I told their parents that their children was doing something illegal and immoral. I told them that what they were doing was invading my privacy online.

They said, "not our angels. They go to church every time the church doors are open." I asked them if I could see the children's computer. They said, "Sure, but you will not find anything." I began to search with a porn system scanner. I told the parents, "come here and look. Here are the same pictures I got from my system. Look and see that these pictures are your children." They were shocked that their little angels was actually junior hackers and cybercriminals. This experience taught me two things. First, do not think your system is squeaky clean because people like the above are out there and ready to cause you trouble. Two, keep your system clean. Mine undergoes a thorough scrubbing at least once a month. Virus software runs continuously, along with the antispyware. I use undelete at least once a week. Lastly do not leave a document unencrypted because there are people out there that will steal you ideas and inventions. Oh, the children were punished by me. I put a copy of a program similar to Netnanny or Cyberpatrol on their system. I've since added this type of software on my system. It warns me when someone tries to put illegal stuff on my computer. I set my privacy controls and use TOR browser. This insures that I have privacy and not be at the mercy of every person online. I told the parents they ought to watch what their children are doing online.

The original book had software suites for antivirus and antispyware. I've become more concerned about government types that use Orwellian laws to get their way. To hang on your stuff is more important than all the antivirus and antispyware suites on earth. Since that time I learned about the NSA spy program. I knew deep down inside that they were up to no good when a person near Salt Lake City said something is up because the government is building something big here.

It does not matter is you are trying to keep Grandma's recipes safe, keeping scanned legal papers safe, or even trying to keep some of your pictures and books safe. All are important to the person having them. I keep some inventions and ideas safe by using this technique. I always keep a back up copy of them because what would happen if your computer's operating system went down. These are kept on external hard drives unhooked from the computer and unplugged from electric.

The Practical Paranoid walked into the room and to the podium. He cut off the microphone and began to speak. He asked, "How many of the audience use encryption? How many encrypt documents, pictures, and other files?" Many raised their hands. He asked, "How many thinks that they have nothing to hide from the authorities?" A third raised their hands. He asked, "How many encrypt documents for a business?" Several raised their hands. He said, "When you get through with this class...you will be able to drive the authorities up the wall. You will be able to take the files anywhere without danger of the authorities getting them. If you think you have nothing to hide then you would probably allow the cops to check your car without a warrant or check your house without a warrant. These people are fools in the highest degree. Take the little quiz that I handed out and we will see how you rank." He handed out a quiz. It can be found in hand outs at the end of this book.

Once finished he asked, "How many answered all of them yes or 7 out of the 12 yes?" A few raised their hands. He said, "I need to talk to you later." He then asked, "How many answered 6 or less Yes." about two thirds raised their hands. He said, "remember, threats can be real or imagined. Trust no one with any of your personal stuff including beliefs. The ones that answered most of these yes are blindly obedient and would be the first to go to camp FEMA if they told them to go for their own safety. I would prefer to take my chances free than to be locked up in a death camp. Blind obedience is dangerous."

DOCUMENT ENCRYPTION

He began his lecture, "When I was a young buck and computers was only used by the government I thought that it would be foolish to encode documents. As time went on and computers had became a common item in the home I believed that my stuff was safe from prying eyes. The cops would never do anything dishonest to discredit a person. I had nothing to hide. One day, I was watching a ballgame when there was a bang on my door. It was the police. As it seemed there was a person trying to destroy me both financially and psychologically. The cops took my computer and began to examine it in the laboratory. After that I got my computer back. The documents had been removed, my pictures had been taken off, and my contact list taken off of it. Anyone that believes that authority is honest is a fool. In this society, be afraid, be very afraid, and be extremely paranoid. We are living in an extremely Orwellian society in which you are watched every day and every minute. We are nothing, but rats in a scientist's cage. First, we will discuss the encryption of documents, pictures and other media. This class will have the same software I have on my home computer. I've took the liberty of adding other freeware programs to the lab's computer. Any questions before we start?"

A woman said, "I know about the authorities pounding on your door. They make the people that ratted you out feel like a hero. They worship these false gods and heroes, but is this class only on encryption?" He replied, "This class is a week long. You will learn how to use scrap hard drives and how to hide them from the authorities. How to clean your drive of garbage. The uses of an undelete program. The advantages and disadvantages of cracked software. How to encrypt documents and how to hide your passwords to your documents. How to create a fake operating system on another scrap hard drive and how to quickly switch out the hard drives. How to create your operating system on a large thumb drive. Imagine you are a rabbit being chased by a fox. We are going to outfox the fox. We will start with the easiest operations first. I see there are quite a few children in this class. What happened? Get expelled for cyberthreatening or something else?" One said, "I am the President of the Student Cybersecurity Club. Our school made arrangements for us to take this week long class." He said, "Security is a very important thing. Privacy and to keep you privacy is also very important. Your protection and preservation of your image is very important. Moral philosophy is not my cup of tea, but remember if you do not protect yourself against all threats both real and imagined then you are in the same league as evil. Let's go to the lab." He opened the door

and said, "Find a machine. I made these from recycled parts. If you want to take them home then you may do so after this class. You may also take the external hard drive and the one hanging on the side and the one sitting on top of the machine. You may also take the Cds and DVDs on the machine. Turn on your machines."

One woman exclaimed, "It says that it cannot boot up. I doesn't have a operating system." He said, "Cut the machine off. Unplug the hard drive and remove it from the holder. Notice the one sitting on the computer. Plug it in and try cutting the machine on. It should work." Everyone's computer came on with the familiar welcome screen from the most popular operating system. He said, "Now we will make a fake system. This is a Decoy to make the cops go away. Cut off your machines. Remove this hard drive and replace it with the one that would not work. Now plug in the modem wire into the back of the machine. Now you have a choice to make. Do you want operating system 1, 2, 3, 4 or 5 on this hard drive? Turn on the machine and open the DVD burner. Insert one of the operating system DVDs. Cut off the machine and cut it back on."

Each person chose a different flavor of the operating system. Finally a woman asked, "What good will having this decoy drive?" The Practical Paranoid said, "The operating systems that you are putting on this drive are very secure. This hard drive is used to write emails to your family, business, and other uses. If you are into criminal activity then using this hard drive for criminal activity will get you into trouble. Everyone may take a walk, get a snack or go smoke if you wish. The operating systems take about 5 minutes for the first part of the install. I need to talk to the blind obedient sheep anyway. The ones that blindly follow." They stayed behind and he said, "I do not go into moral philosophy, but this group blindly follows without question. Remember reading about a dictator that the people blindly followed? What happened? There are also fake diseases that are treated with psychoactive drugs. What happens to the children? They die in their 20s and 30s from heart problems. They are nothing more than drug addicts or speed heads. That will be all. Go."

After five or so minutes all had returned to the laboratory. He said, "I see all had returned. Now you must set the clock on the computer. In other words what time zone are you in. Now you need to set a password to get into this system. Now press <Next> and let the system set up." After 15 minutes all the computers had a new operating system. He said, "This is not the bloatware operating system that is usually given on these computers when you purchase one. Remove the DVD. Turn the machines off, cut it on and log into your new operating system. I am going to show you something special. On each of the DVDs you used to install the operating system. Insert it and copy the TOR zip file onto the desktop. Now unzip this file. This is the gateway into Darknet. Welcome to the dark side. This browser is highly secure. This is the main ones that I use for email, and other communications. Now turn your machines off. Take out this hard drive and insert the thumb drive. Use one of the Cds marked 1a, 2a, or 3a. Do as you had before. We are setting up a thumb drive operating system. This operating system is tiny. It will set up in a few minutes. Once set up then put the drive marked E into the machine and cut it on."

He waited until all everyone had set up the thumb drive operating systems. Everyone put the Drive marked E into the machine and cut them on. He said, "type in "All" into the log in. Anyone have trouble with setting up the operating systems? You may take them with you if you wish. I got them free."

A lady said, "I've never used a computer in my life. This is easy." He replied, "It is easy, but you are living in a world in which is very dangerous. We will start with some safety rules. Never give the password to your system to anyone. Never give your email out to businesses. Never download software that requires a download manager or one that will install the software on your machine. Never use P2P software to get files. All of these are security risks. Always use TOR browser. Never use commercial email services. They promise you the sun, moon, and the stars, but they are also

security risks. They sell your metadata to the feds. Never use encryption or other software that requires you to register it except freeware antivirus, antimalware, and antispyware. All of this is mentioned in the booklet. Now we will go to encryption of documents and pictures."

He said, "Everyone ready? Open the document folder on your machine. These files are fake and represent actual documents for a business. Now we will begin. All this is discussed in the booklet, but we will do this hands on. Encrypt files, Encrypt4all, File Waster and File encryption does not possess a password creator. One can get a freeware one or just simply use cryptolab to do the job for you. Crypt4free can create password, but they are maximum of 15 digits.

Androsa File Protector-This one is good to harden drives, documents and so on.

Algorithms used-DES, TripleDES, Rijndael

Cryptolab-Freeware. Used to create unbreakable passwords, but it is an email encryption program.

Crypt4Free-This one works well on documents, but if you have a list of software files to encrypt for a traveler drive then this software will not work on them. Encrypt files works well on these pieces of software. The free version only allows you to use two algorithms.

Encrypt4all-Although being freeware this one asks you to register it. This is a security risk.

Encrypt files-Freeware. Good solid encryption for files such as wordpad, scanned files, and such.

Encryptonclick-This one is good to harden documents and folders.

File encryption-Freeware. Same as above.

File waster-This one possesses some problems. These will be discussed later."

A woman asked, "Why encrypt files and folders then hardening the folders and files?" He said, "Imagine, you go to work. Your boss asks you to take some very important communications to an office. In the meantime the federal guys stop you and take the information. Sure you have a copy of the information to be delivered, but what if it is not to be read by the government? A hardened drive would solve the problem. If you harden and put in an encrypted drive, harden and repeat the process several times then how difficult would it be for these people to get the information? It would be impossible or very difficult. Imagine putting a virtual minefield of viruses in each of the encrypted drives. What would happen if they were crazy enough to try to open one of these mines? It would shut down their system. Many things such as private pictures, journals, and important scanned papers should not be read by anyone else, but you and whoever is supposed to read them. Now let's get back to using the software. Open File Waster please. Make a copy of the file "Test" in the documents. Click the icon that looks like a folder. Then browse around for the copy of "Test" this file contains pictures, documents, and other files. Put in a password and click the button <encrypt>. Now look in the file. All the names are scrambled and look weird. Reverse the process and look. The files look normal. Everyone got that. Do take notes in the little notebook in back of the booklet."

A girl asked, "Will you help me. I did not get that." He walked over and said, "Look in documents and find "Test" and make a copy. See that little picture. Click it. Now, choose the file "Test." and put that in the file waster. Put in a password in both places and click the far left button. Look in the file and reverse the process. Put the "Test" file back into the file waster window and your password in both of the windows. Click the decrypt button. Got it?" She said, "Yeah." He said, "practice this

when you get home. That DVD contains file waster. Put it on your computer and practice. We will now use androsa file protector. You will need to mark which password goes with these pieces of software. Look in the booklet and it will show you. Now open Androsa File Protector. Press the button that looks like a file. Look for the file "Test" again and click it with the mouse. There will be a list of files pop up from the folder. Press <Portect/Restore> Choose the AES 256 encryption and put in your password as before. Press the protect button. If you repeat the process you restore the files. Very simple to use. We will use all the software on the list. Let's try "Encrypt files" It is simple and heavy duty. Forget about encrypt4all because it nags you to buy it. You will need to hold down the <Ctrl> button and shade all the files in the package. Hit encrypt and it will ask you for a password. Look in OS(C) and click it. There is a tree diagram. Click the middle user in the list. Documents is the next part of the tree you will need to look. Oper "Test" Press <Ctrl> and shade the whole file. Choose your encryption algorithm. Put in the passwords and encrypt. This one works the same as the program "File encryption" a little practice you will do well with it. Now, go into program files on the start menu and look at "2Brightsparks" this is Encrypt-On-Click software. This will encrypt everything in the file. Practice with this software. You will be tested on it, but it is a hands on test. Since we had worked very hard on this software and half the day is gone then we will go to lunch. Meet back here in an hour or at 1:00. We will work on other freeware software."

The crowd milled back into the computer lab. The Practical Paranoid said, "Now, we will use some software that possesses a limited time for use, but we will take pieces from this software and keep them forever. When you all are ready then we will begin. Notice the new recycled hard drive in the plastic bag on your desks. These hard drives had been taken from computers at the last electroinic recycling drive. They are all 500 GB hard drives. Attach these hard drives to the "Cow Tail wire hanging at the side of your computer and plug it in. Cut on the computer. Go into my computer and format this hard drive. Any problems then let me know." He went around and watched them work. He said, "No my dear it is this one. That one contains a copy of your operating system. Format it then you cannot repair your computer. He turned and said, "Be careful. Don't format the wrong drive. Everyone ready. Install Steganos Security Suite. Everyone ready? Ok, go to now start up the software. Hit the button that <Portable Drive> and make two or three portable drives about 100 GB each, but you will need to rename them as they are made. Put them in the hard drive you hooked up. Now make three or four 4 GB portable hard drives on the same hard drive. Each one will need to be renamed. Cut the computer off after these had been made. Disconnect the drive. You can keep these portable drives until the cows come home. I use a large external hard drive when I made mine. I created several that was 56 GB and one 250 GB and a bunch of 4 GB portable drives. They can be copied and be useable. Do record your passwords or you will not be able to open them in the future. I change the passwords on them. Now, tomorrow we will cover the concept of creating portable drives and hardening them. Leave your materials on your desk and we will start on this tomorrow. We covered a massive amount of material. We've practiced file encryption and tomorrow We will take up the subject of creating encrypted and travel drives then hardening these drives thus creating a box in a box scheme. We've already created on type of encrypted drive. Tomorrow we will see which software would be effective in hardening it. I bid you a good evening." Everyone filed out and he locked the door to the windowless laboratory.

ENCRYPTION HARDENING OF A TRAVEL DRIVE

The next morning the class began coming in for the next part of the cryptography class. He said, "good morning. I have an announcement in 15 minutes. Finally he began, "Copy one of the 4 GB portable drives onto the desktop. Shade the file Press <Ctrl> C then go to the desktop and hit <Ctrl V>. When it copies then we will begin to harden it. Let's start with file waster. Now we will decrypt it. Try to open it." Many said it would not open. The Practical Paranoid said, "It is called file deflation. The rest of the encrypted drive is functional, but not the drive itself. Go back to the original and cut the sle file and paste it in the desktop box. It needs to be from the same travel drive.

This is just an experiment. I've never done it. We will see if we can make the travel drive functional again. Now try it. It works, but file waster cannot be used on a steganos portable safe. We will try another one for this purpose. Open Androsa Fileprotector and see if it deflates the sle file. It will take a while for it to work.

We will do this for all the drive software. Harden decrypt the hardening and try to open it. If it fails then write it down in the notebook in the booklet.

File Waster failed in hardening a steganos portable safe. It deflated it.

Androsa Fileprotector is very slow, but it will work. If in a hurry then Androsa would not be a wise choice hardening the drive.

Let's try AxCrypt next. It is a free program. Put in the password and encrypt. Look at all the warnings. Let's try to decrypt it. The entire drive had been destroyed. Try to open it. Opening it failed so, this program cannot be used for hardening. Delete this damaged drive and copy one to the desktop.

Next we will try Bcarchiver for this purpose. Now it wants to generate a public key. I would not recommend this software because it is a security risk.

Now, we will try 7zip. Notice how slow it is working. We can say that we can use it, but how can we be for sure about the damage. In the lower right hand corner there is the encryption for the files. Mark you want to encrypt them and enter a password. We will see what damage is done. This one is not suitable for our purposes. Damage was done to the archive. The program "Sticks" at about 96% decompression." He sat down at his desk in the front and began to play around with the software.

He said, "Class, do not remove the Axcrypt and BC archiver because they work well for documents. The same is true for File Waster and 7 zip."

Let's now try another one Crypt4free seems to be a good one. Choose blowfish for you encryption. It will not encrypt anything. 7Zip would be fine for mixed encryption. Like keeping the decryption program for the drive safe. Using the method using one or more programs is called mixed encryption. Mor about that subject later. Repair your portable drive by cutting and pasting another copy of the sps.sle file in this folder. Encrypt4free also does not work with hardening. I've tested it last night.

Let's try the program called Encrypt files and if there is no damage then try File encryption." He waited and then said, "decrypt the program. Try to open it." Several in the class gasped as the drive mounted, but it could not be displayed. He said, "go into the computer and look at drive Z. Click it. It will display <format drive>. Let's format it and see what happens. It is empty, but you have a smaller safe. Let's go to 2Brightsparks in the programs and see what Encrypt-on-Click will do to this portable drive program. Decrypt it and see. It remains functional. Let's go to lunch. We had been busy. Encrypt-on-Click works. Be back at 1:00 and we will wrap up this session. I will copy off a sheet to take with you. Everyone understands document encryption and some of the basic concepts of hardening a drive. We now know two programs that will encrypt the drives."

MIXED ENCRYPTION

This is simply using two programs to encrypt a travel drive. I will not go into this process because it would be overkill.

LARGER ENCRYPTED DRIVES

The Practical Paranoid said, "Now, since we had covered making the travel drives and using them. We also learned how to harden them. Now, we will use the software that can make only a 4 GB drive and we will use the softwares make drives of any size. The one that can only make one of 4 GB is Secret Drive. The ones that can make drives of any size is Truecrypt, freeOTFE, and Toolwiz Bsafe. Play around with the software to learn how to use it. Sometimes I will harden them as an extra measure of safety.

STEGANOGRAPHY

The Practical Paranoid replied, "Most of the freeware steganography software is a pain to use. I've decided not to go into this area. Why use a software that it would take a great deal of time to use? We are talking about situations in which time is short. We need to get the information hidden quickly. The fastest ways of hiding files is using the methods given. Tomorrow I will give everyone the verdict on a piece of software that you can hide materials in audio and video files without altering the quality of the audio and video. Openpuff is a good program and I will be testing it out tonight. It requires three passwords to open the file. Tomorrow I will tell you if both types of software would be worth getting. I'll bring copies of it if it is worthwhile to have it."

A woman asked, "why use steganography? These programs work fine and they are fast. My husband is a surgeon and he hides his patient records in encrypted drives. A better word is stores records. He tried stegano and he said it is hard to use and very slow. He said open puff is fine if you have some rather large files that could hold the files. I would not suggest using any of the stegano programs. The encryption is a low level and weak." The Practical Paranoid said, "I agree with you and your husband. It is a very low level hiding of information. Stegano is the art of covered or hidden writing using image, audio, or video files. This is the oldest technique known. We will forget about this form of cryptography because it tends to be slow. We need speed and safety and not something that can be uncovered with certain software. Now we will cover a very important idea. Keeping you system clean by undeleting erased files and putting them on an encrypted drive then erasing the drive. This will be covered tomorrow"

He unlocked the laboratory door and said, "everyone be seated. Steganography is not worth using or having. It is difficult to use and the security holes is not worth the hassle."

UNDELETE

The Practical Paranoid came in and said, " Good morning. I see quite a few of the paranoids are still in the class." He handed everyone a plastic bag with a hard drive in it. He said, "Don't worry, these did not cost me one red eyed cent. This will be our garbage can. A thumb or flash drive works just as well. But I can go to the electronic recycling place with a screwdriver and get as many as I want. Hook this on the cow tail on your system. On the system utilities such as Advanced Systemcare and Glary Utilities there are undelete programs, but these the computer must be hooked up to the network. This creates a security risk. Don't use these programs. We will use several free programs to

search for garbage. Think this system is clean? Then think again.

Recuva-This one is good to clean a system, but others will be compared against it to find out how it does under a real world situation. I check all of the files listed and over write them.

Pandora recovery-This one makes a person to connect to the internet. First thing that came to my mind is security threat or security risk. Three out of the five request you to connect. Any person can read what is on your computer with one of these managers if they have the skill.

Easeus-This one caused me to crash my whole system. I recovered all the deleted files and erased the encrypted drive. Not thinking I turned my system off. All I got the next morning was a blank screen. I was lucky that I had cloned the drive before testing it.

The best of this software is Recuva.

All of this is in the booklet."

A woman asked, "Is this why we should take extra precautions with our system? Some of this borders on insanity." He said, "A very wise person told me that it is better to be safe than sorry. He took extra pains when working on anything. I thought he was crazy until one time a building burned in my town. A woman got on a cell phone and her mother was in a different area. She indicated that she stay put until the heroes come to get her. She died from smoke. One person I know before he would work on anything he would make sure it was safe. I heard on the olice scanner that a car had rolled onto a person because he did not make sure it was safe. One guy was arrested in my home town because someone had put child porn on it. The company fixing his computer put the material on it to discredit him. I've had my computer breached and stuff put on it. The two junior hackers was surprised when I was sitting on their front porch after school. The parents basically said their children are angels until I presented them my evidence and put program that would not allow them to put pictures from a thumb drive to their computer without a password. I was never bothered with these kids again. One cannot be too careful. Trust no one. Now, cut on your machine. Turn on Recuva. Use all files setting and hit next. Use the I'm not sure setting. It will also scan the drive you put on the computer. Put all the recovered files on Drive F. Go get coffee or have a smoke because it will take a while to recover them. If you use the deep scan setting it can take quite a while to scan the system. "

They filed back into the classroom. He said, "Now we will forensically delete these files. Forget about using format because they can be recovered. Let's leave these files in Drive F. Let's now discuss how to delete these files so they cannot be recovered. We do not want to destroy our computer. Degaussing is out because it destroys everything. You could use the fake disk, but then you would still have all the garbage on drive F. Let's look at a list of the free cookie and garbage cleaners. If I had a very small hard drive then I would leave these off because Glary System tools and advanced systemcare will do the job. If you really need one then the list below in the booklet will give you all the cleaning ability you will need."

CLEANERS

Privacy Eraser Free

Ccleaner-I've used this one for years.

Jet clean

ERASERS

These are used to wipe the free space on your system. We will use one of these to erase the garbage can drive. Ones I've used are as follows:

Eraser
Secure Eraser
Free eraser
File shredder.

He then said, "Open up the one called Eraser. We are going to set it. Go to settings. Choose Gutmann for both. This is a slow method, but secure. We will now erase the garbage can. Highlight all the files in the garbage can. Do you know how to do the erase. Click the left button on your mouse and Move down the list down to Eraser. Choose erase on the second list. Now that everyone had gotten their system started we can go home. Leave the computers on because it takes several hours for the process to complete. We will discuss the so called secure erase settings on Glary and Advanced Systemcare and on encryption software. Since this is Thursday we will wrap up the class tomorrow and I will give a few more pointers." The class left and he locked the door behind him.

He came in and unlocked the door. He said, "see if the erasing had completed. " All of them had completed the process. He said, "Now, we will wrap everything up. Here are cards to indicate you had completed my class." He handed out the cards. He said, "here are the papers you will need to show that you had completed the class and your qualifications." He said, "how many want to take their computers with them? Most wanted their encryption computer. He said, "remember you are taking a risk with peer-2-peer software. Anytime when using your machine on a network use the TOR browser. Always schedule complete computer cleanup once a month. Use trash cleaners like ccleaner often. Use a little commonsense and you will be safe. Protect your stuff like you would protect your home. Don't learn it the hard way. The hard way can be a tough teacher. How many want to take their machines home with them? They are yours and you can use them at home."

QUIZ

Would you allow a police officer search your car without a warrant?

Would you allow a police officer search your home without a warrant?

Would you allow a police officer search your computer without a warrant?

Do you believe authority figures are your friends?

Do you believe what the news media is telling you?

Do you believe the President, Congress or other people in power?

Do you believe you actually elect the President?

Do you leave your home unlocked?

Do you believe you are powerless with regard to the government?

Do you believe in Globalism?

Do you believe what the scientific community is telling you?

If a doctor told you to take a lethal medicine you would take it?

Don't confuse this with the travel drive software. The ones that I use and harden them are the ones below:

Use for hardening

Androsa File Protector.

Encrypt-on-Click

Drive making software

freeOTFE-This one can be deflated with the chkdsk on Windows.

Truecrypt-They say there are security problems with it. Harden it and then security would not be the problem.

Labvault-I've jsut downloaded this software and will be testing it

Bitlocker-Another good program when hardened.

Toolwiz Bsafe-I've used this one when the first version came out.

PGP free-I've used this one for years.

Secret Drive-I've used this one for years, but it only creates a 4 GB drive. This is fine if you are collecting movies and putting all the remakes together.

TRAVEL DRIVES

There are only two that I would recommend.

Steganos Portable Safe

Discryptor

MIXED ENCRYPTION

Mixed encryption is the use of one or more encryption programs to encrypt a travel drive.

To encrypt the drive file of the program there are two programs that will work. The drive file is the largest file in the set. Put it in a folder called drive. Pur the rest of the program in a file called decryption program. Do keep this in the main file folder.

Ones that will encrypt the drive:

Androsa file protector

Encrypt-on-click

For encryption of the rest:

File zip tools that allow for encryption.

Encrypt files (suggested)
File encryption (suggested)
File waster
Smart Encyyptor
CryptoEx is next to worthless
Cypherix (don't use)
Encrypt4all